

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

PEGGY CHRISTEN and)	
JOSEPH T. COUGHLIN, individually)	Civil Action No.:
and on behalf of all others similarly)	
situated,)	
)	
Plaintiffs,)	CLASS ACTION
)	
v.)	JURY TRIAL DEMANDED
)	
EQUIFAX INC.,)	
)	
Defendant.)	

CLASS ACTION COMPLAINT

Plaintiffs, Peggy Christen and Joseph T. Coughlin (“Plaintiffs”), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant, Equifax Inc. (“Equifax”).

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Equifax for its failure to secure and safeguard the private information of approximately 143 million Americans.

2. On July 29, 2017, Equifax discovered unauthorized access to databases storing the confidential and private consumer information of millions of U.S. consumers.

3. On September 7, 2017, Equifax publicly announced that due to vulnerability in its systems, its files were accessed by criminals for at least the period of mid-May through July of 2017 the (“Security Breach”). The information accessed includes names, Social Security numbers, birth dates, addresses, and driver’s license numbers, in addition to credit card numbers

for some consumers and other documents containing personal identity information (“the Private Information”).

4. Plaintiffs and Class members’ Private Information was accessed and stolen by hackers in the Security Breach.

5. Equifax’s security failures enabled and facilitated the criminals’ access, obtainment, theft, and misuse of Plaintiffs’ and Class members’ Private Information. Unauthorized persons gained access to Equifax’s databases through vulnerabilities in its security and executed commands that caused the system to transmit to the unauthorized persons electronic data comprising millions of Americans’ Private Information. Equifax’s security failures also put Plaintiffs and Class members at serious, immediate, and ongoing risk of identity theft, and additionally, will cause costs and expenses to Plaintiffs and Class members attributable to responding, identifying, and correcting damages that were reasonably foreseeable as a result of Equifax’s willful and negligent conduct.

6. The Security Breach was caused and enabled by Equifax’s knowing violation of its obligations to secure consumer information. Equifax failed to comply with security standards and allowed the Private Information of millions collected by Equifax to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach.

7. Accordingly, Plaintiffs, on behalf of themselves and all others similarly situated, assert claims for violation of the Fair Credit Reporting Act, violation of the New Jersey Consumer Fraud Act, and all other substantially similar statutes enacted in other states, and negligence. Plaintiffs seek monetary damages, punitive damages, statutory damages, and injunctive relief, and all other relief as authorized in equity and by law.

II. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiffs' Fair Credit Reporting Act claims arise under the laws of the United States.

9. This Court also has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds \$5,000,000, exclusive of interest and costs.

10. This Court has personal jurisdiction over Equifax because Plaintiffs' claims arise out of Equifax's contacts with New Jersey.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District.

III. PARTIES

12. Plaintiff, Peggy Christen ("Christen"), resides in North Plainfield, New Jersey, and is a citizen of the State of New Jersey. After learning of the Security Breach, Christen used a tool on Equifax's website to determine whether her Private Information was affected. Using this tool, Christen determined that her private information was affected by the Security Breach. As a result of the Security Breach, Christen suffered from the deprivation of the value of her Private Information and will incur future costs and expenditures of time to protect herself from identity theft.

13. Plaintiff, Joseph T. Coughlin ("Coughlin"), resides in Cranford, New Jersey, and is a citizen of the State of New Jersey. After learning of the Security Breach, Coughlin used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Coughlin determined that his private information was affected by the Security Breach. As a

result of the Security Breach, Coughlin suffered from the deprivation of the value of his Private Information and will incur future costs and expenditures of time to protect himself from identity theft.

14. Defendant Equifax is a nationwide consumer reporting agency and purveyor of credit monitoring and identity theft protection services. Equifax is a Georgia corporation headquartered in Atlanta, Georgia.

IV. FACTUAL BACKGROUND

15. Equifax is in the business of collecting, assessing, and maintaining the Private Information of approximately 800 million consumers around the world in order to sell this information to third parties in the form of consumer credit reports, consumer insurance reports, or consumer demographic or analytics information. It also sells credit protection and identity theft monitoring services to consumers.

16. In the years preceding Equifax's announcement of the Security Breach, several entities storing large quantities of consumer data caused massive security breaches, including health insurer Anthem, Yahoo, Equifax's competitor, Experian, and many others. Equifax knew or should have known that the Private Information contained in its databases was a prime target for hackers. In fact, it makes many millions of dollars in profits convincing Americans to buy its credit protection and identity theft monitoring services to guard against such breaches and the damages they cause. Despite this, Equifax failed to take adequate steps to secure its systems.

The Equifax Security Breach

17. On September 7, 2017, Equifax announced that its systems were compromised by cybercriminals, reportedly impacting approximately 143 million U.S. consumers. The Security Breach began in mid-May, 2017, and was not detected by Equifax for several months. Equifax admits the Security Breach arose from a "U.S. website application vulnerability" in its systems.

18. Unauthorized persons manipulated Equifax's security vulnerabilities to gain access databases of consumer information. Equifax's systems transmitted to the unauthorized persons during a period of time of over two months without Equifax detecting or limiting the infiltration.

19. After Equifax discovered the Security Breach on July 29, 2017, it waited more than six weeks before it began notifying impacted consumers on September 7, 2017.

20. In response to the Security Breach, Equifax falsely claims to provide "complimentary identity theft protection and credit monitoring" through the website they created: equifaxsecurity2017.com.

21. In fact, this service is not complimentary and it is not adequate. It is being offered in exchange for waiving significant legal rights, including the Constitutional right to a jury trial, as described in the fine print on the hyperlinked "terms" page, which, among other things, purports to bind users to individual arbitration.¹

22. The consumer information compromised in the Security Breach includes names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and documents containing personal identity information—all information that is now in the hands of criminals.

Security Breaches Lead to Identity Theft

23. According the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.²

¹ *Terms of Use*, available at <http://www.equifax.com/terms/> (last visited Sept. 8, 2017).

² See *Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Sept. 8, 2017).

24. The Federal Trade Commission (“FTC”) cautions that identity theft wreaks havoc on consumers’ finances, credit history and reputation and can take time, money, and patience to resolve.³ Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.⁴

25. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for a number of years.⁵ As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

26. In fact, “[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud.”⁶

The Monetary Value of Privacy Protections and Private Information

27. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information:

³ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf> (last visited Sept. 8, 2017).

⁴ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” *Id.*

⁵ Companies, in fact, also recognize Private Information as an extremely valuable commodity akin to a form of personal property. See John T. Soma et al., *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PERSONAL INFORMATION”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

⁶ *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at <http://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/> (last visited Sept. 8, 2017).

The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.⁷

28. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a \$26 billion per year online advertising industry in the United States.⁸ Indeed, as a nationwide consumer reporting agency, Equifax's entire line of business depends on the fact that the Private Information of consumers is valuable, both individually and in aggregate.

29. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.⁹

30. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will

⁷ Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Sept. 8, 2017).

⁸ See Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Sept. 8, 2017).

⁹ *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited Sept. 8, 2017).

make a profit from their Private Information.¹⁰ This business has created a new market for the sale and purchase of this valuable data.¹¹

31. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was \$1,349.”¹²

32. The value of Plaintiffs’ and Class members’ Private Information on the black market is substantial. By way of the Security Breach, Equifax has deprived Plaintiffs and Class members of the substantial value of their Private Information.

Damages Sustained by Plaintiffs and Class Members

33. Plaintiffs and Class members have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Private Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market—for which they are entitled to compensation.

34. Plaintiffs and Class members have suffered additional damages based on the opportunity cost and value of time that Plaintiffs and Class members have been forced to expend to monitor their financial accounts as a result of the Security Breach.

¹⁰ Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, <http://www.nytimes.com/2010/07/18/business/18unboxed.html> (last visited Sept. 8, 2017).

¹¹ See *Web’s Hot New Commodity: Privacy*, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Sept. 8, 2017).

¹² See Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Sept. 8, 2017).

35. Acknowledging the damage to Plaintiffs and Class members, Equifax is instructing consumers to “be vigilant in reviewing their account statements and credit reports,” “immediately report any unauthorized activity to their financial institutions” and to “monitor their personal information.” Plaintiff and Class members now face a greater risk of identity theft.

V. CLASS ACTION ALLEGATIONS

36. Plaintiffs bring all counts, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as:

All persons whose Private Information was affected by the Security Breach that occurred from at least mid-May 2017 through July 2017, including all persons who Equifax’s “Check Potential Impact” tool identifies as being affected.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

37. In the alternative, Plaintiffs bring all counts set forth below on behalf of themselves and statewide classes with laws similar to New Jersey law, or further in the alternative, a New Jersey class (collectively, these alternative classes are referred to as the “New Jersey Class”) defined as:

All persons in New Jersey (and in those states with laws similar to the applicable law of New Jersey) whose Private Information was affected by the Security Breach that occurred from at least mid-May 2017 through July 2017, including all persons who Equifax’s “Check Potential Impact” tool identifies as being affected.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

38. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as

would be used to prove those elements in individual actions alleging the same claims.

39. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number over one hundred million. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Equifax's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

40. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. Whether Equifax failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' Private Information;
- b. Whether Equifax properly implemented its purported security measures to protect Plaintiffs' and Class members' Private Information from unauthorized capture, dissemination, and misuse;
- c. Whether Equifax took reasonable measures to determine the extent of the Security Breach after it first learned of same;
- d. Whether Equifax willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Private Information;
- e. Whether Equifax was negligent in failing to properly secure and protect Plaintiffs' and Class members' Private Information;
- f. Whether Plaintiffs and Class members are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

41. Equifax engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

42. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of Class members because, among other things, all Class members were comparably injured through Equifax's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Equifax that are unique to Plaintiffs.

43. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of Class members he seeks to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. Class' members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

44. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Equifax, so it would be impracticable for Class members to individually seek redress for Equifax's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision

by a single court.

VI. CLAIMS

COUNT I

Willful Failure to Comply with the Fair Credit Reporting Act, 15 U.S.C. § 1681n

45. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

46. Equifax is a consumer reporting agency and is subject to the requirements of the federal Fair Credit Reporting Act.

47. Plaintiffs' and Class members' Private Information are consumer reports under FCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

48. FCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. 15 U.S.C. § 1681b. FCRA also requires that:

Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

15 U.S.C. § 1681e.

49. Defendant willfully, knowingly, or with reckless disregard, failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b when it enabled and facilitated the Security Breach. Defendant failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

50. Defendant willfully, knowingly, or with reckless disregard, failed to comply with the FCRA's requirements with respect to Plaintiffs and Class members. As a result of Defendant's failures, Defendant transmitted Plaintiffs' and Class members' Private Information to criminals for illegitimate and unauthorized purposes.

51. As a further direct and foreseeable result of Defendant's willful noncompliance with FCRA, Plaintiffs' and Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

52. Plaintiffs and Class members seek any actual damages they have sustained, or in the alternative not less than \$100 and not more than \$1,000 in statutory damages; punitive or treble damages as the court may allow, the costs of this action together with reasonable attorney's fees as determined by the court.

COUNT II
Negligent Failure to Comply with Fair Credit Reporting Act, 15 U.S.C. § 1681o

53. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

54. Defendant negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b when it enabled and facilitated the Security Breach. Defendant failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

55. Plaintiffs' and Class members' Private Information was wrongfully furnished to criminals as a direct and foreseeable result of Defendant's negligent failure to adopt and maintain such reasonable procedures.

56. As a direct and foreseeable result, Plaintiffs' and Class members' consumer reports were accessed, made accessible to, stolen, furnished, and sold to unauthorized third parties for illegitimate and unauthorized purposes.

57. As a result of Defendant's negligent violations of FCRA, as described above, Plaintiffs and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

58. Plaintiff and Class members, therefore, are entitled to compensation for their actual damages, as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o(a).

COUNT III
Unlawful Practices in Violation of the New Jersey Consumer Fraud Act,
N.J.S.A. § 56:8-2, et seq.

59. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

60. Plaintiffs and members of the Class were subjected to Defendant's unfair or deceptive acts or practices, in violation of the New Jersey Consumer Fraud Act ("NJCFA") N.J.S.A. § 56:8-2, et seq., in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

61. Under the NJCFA, the following qualifies as an unlawful practice:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.

N.J.S.A. § 56:8-2.

62. In enacting the Identity Theft Prevention Act, which among other things, amended the NJCFA, the New Jersey Legislature found that "[i]dentity theft is an act that

violates the privacy of our citizens and ruins their good names: victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories.” N.J.S.A. § 56:11-45.

63. Defendant willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

64. Defendant benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

65. Defendant’s failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiffs and the Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

66. Defendant’s conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

67. Plaintiffs and Class members have suffered actual ascertainable losses including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

68. Plaintiffs’ and the Class members’ injuries and losses were proximately caused by Defendant’s violations of the NJCFA, which was conducted with reckless indifference toward the rights of others, such that an award of treble damages is warranted.

69. Defendant’s actions constitute a knowing, concealment, suppression, or omission in violation of N.J.S.A. § 56:8-2.

70. As a result of the foregoing, Plaintiffs and Class Members suffered and will continue to suffer ascertainable losses and other damages as described in detail in the preceding paragraphs of this Complaint, and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

COUNT IV
Violations of New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2, et seq.,
Deceptive and Unfair Business Practices

71. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

72. Defendant falsely represent to Plaintiffs Class members that Defendant offers complimentary one-year enrollment of its Trusted ID Premier product for affected persons.

73. In actuality, Defendant purports to bind persons who enroll in the service to a set of terms, posted on its website, which include a binding arbitration provision. As a result, Defendant's offer is not complimentary and employs deception and coercion in an unconscionable effort to bind affected persons to arbitrate their claims.

74. Plaintiffs and Class members seek an injunction against Defendant from making misrepresentations during the course of attempting to comply with its legal obligations to notify affected individuals.

75. Plaintiffs and Class members seek a declaration that any avilment of Defendant's purportedly complimentary credit protection services do not waive claims against Defendant or otherwise bind or constitute consent or agreement in any way.

COUNT V
Failure to Expediently Notify Following Security Breach in Violation of the New Jersey
Consumer Fraud Act, N.J.S.A. 56:8-2 et seq.

76. Plaintiffs repeat and re-allege the preceding paragraphs as if fully set forth herein.

77. As stated above, the NJCFA provides that it is “an unlawful practice and a violation of P.L. 1960 c. 39 (C.56:8-1 *et seq.* to willfully, knowingly or recklessly violate” Sections 56:8-161-164 of that Act.

78. Section 56:8-163 of the NJCFA requires that a business conducting business in New Jersey:

Shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

N.J.S.A. § 56:8-163.

79. The NJCFA defines a breach of security as follows:

“Breach of security” means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56:8-161.

80. Defendant’s disclosure on September 7, 2017 regarding the breach of security to Plaintiffs and Class Members after learning of the breach as early as July 2017 was delayed and not made in the most expedient time possible.

81. As a result of the foregoing, Plaintiffs and Class Members suffered and will continue to suffer ascertainable losses and other damages and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

COUNT VI
Negligence

82. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

83. Equifax owed numerous duties to Plaintiffs and the other members of the Class.

These duties include the duty:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. to protect Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and
- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class members of the Security Breach.

84. Equifax knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems. Equifax knew of the many breaches that targeted other entities in the years preceding the Security Breach.

85. Equifax knew or should have known that its systems did not adequately safeguard Plaintiffs and the Class members' Private Information.

86. Equifax breached the duties it owed to Plaintiffs and Class members in several ways, including:

- d. by failing to implement adequate security systems, protocols and practices sufficient to protect customer Private Information and thereby creating a foreseeable risk of harm;
- e. by failing to comply with the minimum industry data security standards; and
- f. by failing to timely and accurately discovery and disclose to customers that their Private Information had been improperly acquired or accessed.

87. But for Equifax's wrongful and negligent breach of the duties it owed to Plaintiffs and Class members, their Private Information would not have been compromised.

88. The injury and harm that Plaintiffs and Class members suffered was the direct and proximate result of Equifax's negligent conduct.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this Complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Equifax, as follows:

- A. Certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel;
- B. Ordering Equifax to pay actual damages to Plaintiffs and Class members;
- C. Entering an injunction against Equifax, prohibiting the deceptive conduct described in Count IV;
- D. Ordering Equifax to pay statutory damages to Plaintiffs and the other members of the Class;
- E. Ordering Equifax to pay punitive damages, as allowable by law, to Plaintiffs and members of the Class;
- F. Ordering Equifax to pay attorneys' fees and litigation costs to Plaintiffs;
- G. Ordering Equifax to pay both pre- and post-judgment interest on any amounts awarded as allowable by law; and
- H. Ordering such other and further relief as may be just and proper.

Date: September 11, 2017

Respectfully submitted,

WILENTZ, GOLDMAN & SPITZER

By /s/ Kevin P. Roddy
KEVIN P. RODDY (ID# 014802005)
PHILIP A. TORTORETI

90 Woodbridge Center Drive, Suite 900
Woodbridge, NJ 07095
Telephone: (732) 636-8000
Facsimile: (732) 726-6686
E-mail: kroddy@wilentz.com
ptortoreti@wilentz.com

-and-

ANDREW GROUS
110 William Street, 26th Floor
New York, NY 10038
Telephone: (212) 267-3091
Facsimile: (212) 267-3828
E-mail: agrous@wilentz.com

BEN BARNOW
BARNOW & ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
E-mail: b.barnow@barnowlaw.com

Attorneys for Plaintiffs